

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-95984

(43)公開日 平成11年(1999)4月9日

(51)Int.Cl.⁶
G 0 6 F 7/58
G 0 9 C 1/00

識別記号
6 5 0

F I
G 0 6 F 7/58
G 0 9 C 1/00

C
6 5 0 B

審査請求 有 請求項の数14 FD (全 15 頁)

(21)出願番号 特願平9-276517

(22)出願日 平成9年(1997)9月24日

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 島田 道雄

東京都港区芝五丁目7番1号 日本電気株式会社内

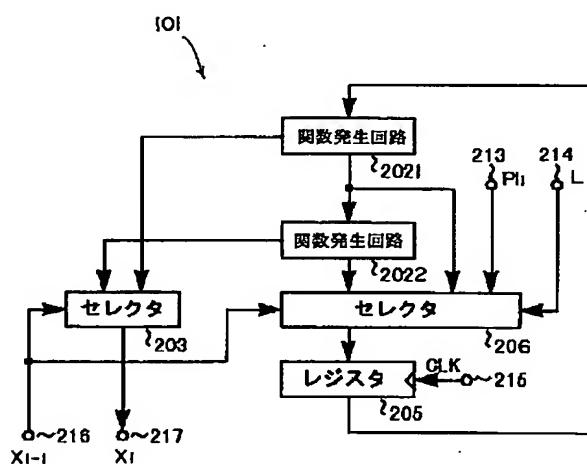
(74)代理人 弁理士 野田 茂

(54)【発明の名称】 摳似乱数発生方法および装置

(57)【要約】

【課題】 暗号学的に安全性の高い撋似乱数を容易に発生できるようにする。

【解決手段】 摳似乱数発生回路101のレジスタ205は、複数のビットから成る状態データを、クロック信号CLKの各クロックバルスに同期して取り込んで保持し、関数発生回路2021、2022はレジスタ205が保持している状態データに応じてそれぞれ複数のビットから成るデータを出力する。そしてセレクタ203は上記関数発生回路がそれぞれ出力する2つのデータのうちのいずれかのデータの特定のビットを、前段の撋似乱数発生回路が発生した撋似乱数 X_{i-1} にもとづいて選択し撋似乱数 X_i として出力する。一方、セレクタ206は上記関数発生回路がそれぞれ出力するデータのうちのいずれかのデータの、上記特定のビットを除いたデータを、前段の撋似乱数発生回路が発生した撋似乱数 X_{i-1} にもとづいて選択しレジスタ205に状態データとして供給する。



BEST AVAILABLE COPY

【特許請求の範囲】

【請求項1】 順序づけられた複数の擬似乱数発生回路を用い、前段の前記擬似乱数発生回路が発生した第1の擬似乱数にもとづいて各擬似乱数発生回路に第1の擬似乱数を発生させ、前記複数の擬似乱数発生回路が発生した前記第1の擬似乱数により第2の擬似乱数を発生する擬似乱数発生方法において、

各擬似乱数発生回路では、

複数のビットから成る状態データを保持し、

保持した前記状態データに応じて複数のビットから成る第1および第2のデータを発生し、

前記第1および第2のデータのうちのいずれかのデータの特定のビットを、前段の前記擬似乱数発生回路が発生した前記第1の擬似乱数にもとづいて選択し前記第1の擬似乱数として出力し、

前記第1および第2のデータのうちのいずれかのデータの、前記特定のビットを除いたデータを、前段の前記擬似乱数発生回路が発生した前記第1の擬似乱数にもとづいて選択し次に保持すべき前記状態データとする、

ことを特徴とする擬似乱数発生方法。

【請求項2】 保持した前記状態データに応じて複数のビットから成る順序づけられた複数のデータを発生し、前記複数のデータのうちの1番目のデータは保持した前記状態データから直接発生し、2番目以降のデータはそれぞれ1つ前のデータから発生し、

前記第1のデータは前記複数のデータのうちの最後のデータを除くいずれかのデータであり、

前記第2のデータは前記複数のデータのうちの最後のデータである、

ことを特徴とする請求項1記載の擬似乱数発生方法。

【請求項3】 S_0, S_1 を $0 < S_0 < S_1$ を満たす整数として前記第1のデータは前記複数のデータのうちの S_0 番目のデータであって前記第2のデータは S_1 番目の前記データであり、

i を1以上の整数として i 番目の前記擬似乱数発生回路が発生する前記第1の擬似乱数の系列の周期を L_i とし、

i 番目の前記擬似乱数発生回路が発生する前記第1の擬似乱数の系列の1周期中に出現する論理“1”的数を W_i とし、

任意の i に対して L_i と $(L_{i-1} - W_{i-1}) \times S_0 + W_{i-1} \times S_1$ とが互いに素で、2より大きい任意の i に対して L_i と $L_1 \times L_2 \times \cdots \times L_{i-2}$ とが互いに素である、

ことを特徴とする請求項2記載の擬似乱数発生方法。

【請求項4】 前記複数の擬似乱数発生回路により発生した前記第1の擬似乱数の排他的論理和を算出し、算出結果を前記第2の擬似乱数とすることを特徴とする請求項1記載の擬似乱数発生方法。

【請求項5】 前記複数の擬似乱数発生回路のそれぞれに対応させて排他的論理和回路を設け、

各排他的論理和回路には、対応する前記擬似乱数発生回路が発生した前記第1の擬似乱数と、前段の前記擬似乱数発生回路に対応する前記排他的論理和回路が算出した擬似乱数との排他的論理和を算出させ、

最後の前記擬似乱数発生回路に対応する前記排他的論理和回路に算出させた擬似乱数を前記第2の擬似乱数とする、

ことを特徴とする請求項1記載の擬似乱数発生方法。

【請求項6】 前記特定のビットは1つまたは複数のビットから成ることを特徴とする請求項1記載の擬似乱数発生方法。

【請求項7】 前記擬似乱数発生回路は非線型擬似乱数発生回路であることを特徴とする請求項1記載の擬似乱数発生方法。

【請求項8】 順序づけられた複数の擬似乱数発生回路を備え、各擬似乱数発生回路は前段の前記擬似乱数発生回路が発生した第1の擬似乱数にもとづいて第1の擬似乱数を発生し、前記複数の前記擬似乱数発生回路が発生した前記第1の擬似乱数により第2の擬似乱数を発生する擬似乱数発生装置において、

各擬似乱数発生回路は、

複数のビットから成る状態データを、クロック信号の各クロックパルスに同期して取り込んで保持するレジスタと、

前記レジスタが保持している前記状態データに応じて複数のビットから成る第1および第2のデータをそれぞれ出力する第1および第2の関数発生回路と、

前記第1および第2の関数発生回路がそれぞれ出力する前記第1および第2のデータのうちのいずれかのデータの特定のビットを、前段の前記擬似乱数発生回路が発生した前記第1の擬似乱数にもとづいて選択し前記第1の擬似乱数として出力する第1のセレクタと、

前記第1および第2の関数発生回路がそれぞれ出力する前記第1および第2のデータのうちのいずれかの前記データの、前記特定のビットを除いたデータを、前段の前記擬似乱数発生回路が発生した前記第1の擬似乱数にもとづいて選択し前記レジスタに前記状態データとして供給する第2のセレクタと、
を備えたことを特徴とする擬似乱数発生装置。

【請求項9】 前記レジスタが保持している状態データに応じて複数のビットから成るデータをそれぞれ出力する順序づけられた複数の関数発生回路を含み、

1番目の前記関数発生回路は前記レジスタが保持している前記状態データに直接したがって前記データを出力し、2番目以降の前記関数発生回路はそれぞれ1つ前の前記関数発生回路が出力したデータにしたがって前記データを出力し、

前記第1の関数発生回路は前記複数の関数発生回路のうちの最後の関数発生回路を除くいずれかの関数発生回路であり、

第2の前記関数発生回路は前記複数の関数発生回路のうちの最後の関数発生回路である。

ことを特徴とする請求項8記載の擬似乱数発生装置。

【請求項10】 S_0, S_1 を $0 < S_0 < S_1$ を満たす整数として前記第1の関数発生回路は前記複数の関数発生回路のうちの S_0 番目の関数発生回路であって前記第2の関数発生回路は S_1 番目の関数発生回路であり、

i を1以上の整数として i 番目の前記擬似乱数発生回路が発生する前記第1の擬似乱数の系列の周期を L_i とし、

i 番目の前記擬似乱数発生回路が発生する前記第1の擬似乱数の系列の1周期中に出現する論理“1”的数を W_i とし、

任意の i に対して L_i と $(L_{i-1} - W_{i-1}) \times S_0 + W_{i-1} \times S_1$ とが互いに素で、2より大きい任意の i に対して L_i と $L_1 \times L_2 \times \cdots \times L_{i-2}$ とが互いに素である、

ことを特徴とする請求項9記載の擬似乱数発生装置。

【請求項11】 前記複数の擬似乱数発生回路がそれぞれ発生した前記第1の擬似乱数の排他的論理和を算出して前記第2の擬似乱数として出力する排他的論理和回路を備えたことを特徴とする請求項8記載の擬似乱数発生装置。

【請求項12】 前記複数の擬似乱数発生回路のそれぞれに対応する排他的論理和回路を有し、

各擬似乱数発生回路に対応する前記排他的論理和回路の一方の入力端子には対応する前記擬似乱数発生回路が発生した前記第1の擬似乱数が供給され、もう一方の入力端子は前段の前記擬似乱数発生回路に対応する排他的論理和回路の出力端子に接続され、

最後の前記擬似乱数発生回路に対応する前記排他的論理和回路から前記第2の擬似乱数が出力される、

ことを特徴とする請求項8記載の擬似乱数発生装置。

【請求項13】 前記特定のビットは1つまたは複数のビットから成ることを特徴とする請求項8記載の擬似乱数発生装置。

【請求項14】 前記擬似乱数発生回路は非線型擬似乱数発生回路であることを特徴とする請求項8記載の擬似乱数発生装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は擬似乱数の発生方法および装置に関するものである。

【0002】

【従来の技術】 1つの擬似乱数発生回路に供給されるクロック信号を別の擬似乱数発生回路の出力する擬似乱数に依存して操作することは古くから行われており、第2次世界大戦中の機械式暗号にまで起源を遡ることができる。また、日本軍の暗号の専門家であった加藤正隆が著した「基礎暗号学」（1989年サイエンス社発行）にも、M系列発生器の出力を間引くことによって良質な擬

似乱数を発生できることが記述されている。しかしながら、クロック信号を操作する擬似乱数発生装置には理論的な解析が難しいという問題があった。

【0003】 このため、理論的に評価されているのは、後述の「段数の等しい線形フィードバック・シフトレジスタ（LFSR）」（特にM系列発生器と呼ばれるLFSR）をカスケード接続した擬似乱数発生装置（図7）に限られていた。しかしながら、このような従来の擬似乱数発生装置には、ロックインの問題があり、ロックインを利用した暗号解読を防ぐために、多数のLFSRをカスケード接続しなければならないという欠点があった。

【0004】 ロックインの問題とは、初段のLFSRが出力する擬似乱数にもとづいて発生されたクロック制御信号によっては、連続する複数のクロックの期間にわたって次段のLFSRにクロックが供給されなくなる場合があり、その際、残りのLFSRも動作を停止してしまい、擬似乱数発生装置が输出する擬似乱数がこの期間中同じ値をとってしまうという問題である。なお、この問題および関連する事柄については、例えば、ゴルマンとチャンバーズの著した論文「クロック・コントロールド・シフトレジスターズ：ア・レビュー」（Dietrich Gollmann and William G. Chambers, "Clock-Controlled Shift Registers: A Review", IEEE Journal on Selected Areas in Communications, Vol. 7, No. 4, pp. 525-533, May 1989）や、シュナイアによる

「アプライド・クリプトグラフィー」（Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, John Wiley & Sons, 1996）などの書籍に詳しく解説されている。

【0005】 図7は、擬似乱数発生回路として線形フィードバック・シフトレジスタ（LFSR）をカスケード接続した従来の擬似乱数発生装置の基本構成を示す機能ブロック図である。図に示したように、この擬似乱数発生装置は順番に配列された n （ n は正の整数）のLFSR902を備え、各LFSR902はそれぞれ m ビット（ m は正の整数）の内部状態を持っている。そして、 i 番目（ i は正の整数）のLFSR902は、入力端子104に供給されている制御信号 L の値が論理“0”的時には、 i 番目の論理和回路901からクロック信号が供給されたら、入力端子105から供給される $n \times m$ ビットのビット列のうち m ビットのビット列を取り込んで内部状態として保持し、一方、入力端子104に供給されている制御信号 L が論理“1”的時には、上記論理和回

路901からクロック信号が供給されることに、内部状態を1クロックパルス分だけ進めるとともに、発生した擬似乱数 X_i （1ビット）を出力する。

【0006】 i 番目の排他的論理回路802は、擬似乱数 X_i と、 $i-1$ 番目の排他的論理回路802が出力する擬似乱数 Y_{i-1} との排他的論理和を計算し、計算結果として得られる擬似乱数 Y_i を、クロック制御信号として $i+1$ 番目のLFSR902に供給すると共に $i+1$ 番目の排他的論理回路802に供給する。なお、最後の排他的論理回路802は、排他的論理和の計算結果として得られる擬似乱数 Y_n をこの擬似乱数発生装置の出力として出力端子106より出力する。

【0007】 i 番目の論理回路901は、入力端子103から供給されるクロック信号CLKとクロック制御信号 Y_{i-1} との論理和を計算して計算結果を出力するので、クロック制御信号 Y_{i-1} の論理値が論理“0”であれば、論理回路901は入力端子103から供給されたクロック信号をそのまま出力するが、クロック制御信号 Y_{i-1} が論理“1”であれば、入力端子103から供給されたクロック信号はこの論理回路901で阻止される。そのため、クロック制御信号 Y_{i-1} が論理“0”的時には、入力端子103からクロック信号が供給されると、 i 番目のLFSR902の内部状態が更新されるが、クロック制御信号 Y_{i-1} が論理“1”的時には、入力端子103からクロック信号が供給されても、このLFSR902の内部状態は更新されない。なお、クロック制御信号 Y_0 は予め決められた定数であり、例えば $Y_0=0$ とする。

【0008】ここで図7の擬似乱数発生装置などを構成するために用いる従来の擬似乱数発生回路について詳しく説明しておく。図8は従来の基本的な構成の擬似乱数発生回路の一例を示す機能ブロック図である。図において、レジスタ205は、入力端子315からクロック信号CLKが供給されると、セレクタ204が出力するmビットのデータを内部状態を表すデータとして保持し、同時に保持したデータを関数発生回路202に供給する。関数発生回路202は、レジスタ205から供給されるmビットのデータに対して予め決められた変換を施し、1ビットを加えて合計 $m+1$ ビットのデータを発生する。そして、このデータの $m+1$ ビットのうちのmビットをセレクタ204に供給し、一方、残りの1ビットは擬似乱数として出力端子317から出力する。

【0009】セレクタ204は、入力端子314に供給されている制御信号しが論理“0”的時には、入力端子313に供給されているmビットのデータを選択して出力し、一方、入力端子314に供給されている制御信号しが論理“1”的時には、関数発生回路202が出力するmビットのデータを選択して出力する。この擬似乱数発生回路では、関数発生回路202はレジスタ205の現在の内部状態を表すデータを変換して出力し、レジス

タ205は、通常の動作状態においてクロック信号CLKの各クロックパルスが入力されるごとに、セレクタ204を通じて関数発生回路202が出力するデータを取り込んで保持する。したがって、各クロックパルスが入力されるごとに内部状態が変化し、変化した内部状態にもとづいて関数発生回路202は擬似乱数を発生して端子317から出力する。

【0010】図9は、特に非線形フィードバック・シフトレジスタと呼ばれる従来の擬似乱数発生回路の基本構成を示す機能ブロック図である。図中、図8と同一の要素には同一の符号が付されており、それらに関する説明はここでは省略する。この擬似乱数発生回路は、関数発生回路202の構成において上述した擬似乱数発生回路と異なっている。すなわちこの擬似乱数発生回路では、関数発生回路202は関数発生回路401およびシフタ402により構成されている。関数発生回路401は、mビットの入力データに対して1ビットのデータを出力するものであり、出力データはシフタ402に供給すると共に、出力端子317を通じて擬似乱数として出力する。シフタ402は、レジスタ205から供給されるmビットのデータを右に1ビットシフトさせて左側の $m-1$ ビットを取り出し、さらに、最左端に関数発生回路401からの1ビットの出力データを付加してmビットのデータとした上でセレクタ204を通じてレジスタ205に供給する。

【0011】したがってこの擬似乱数発生回路でも、関数発生回路202はレジスタ205の現在の内部状態を表すデータを、関数発生回路401およびシフタ402の作用によって変換して出力し、レジスタ205は、通常の動作状態においてクロック信号CLKの各クロックパルスが入力されるごとに、セレクタ204を通じて関数発生回路202が出力するデータを取り込んで保持する。したがって、各クロックパルスが入力されるごとに内部状態が変化し、変化した内部状態にもとづいて関数発生回路202は擬似乱数を発生して端子317から出力する。

【0012】図10は、図7の擬似乱数発生装置を構成する線形フィードバック・シフトレジスタの基本構成を示す機能ブロック図である。図中、図8、図9と同一の要素には同一の符号が付されており、それらに関する説明はここでは省略する。図10に示したLFSR902は、関数発生回路401が排他的論理回路501により構成されている点で図9の擬似乱数発生回路と異なっている。排他的論理回路501は、レジスタ205からのデータを構成するmビットのうち予め決められた複数ビットの排他的論理和を算出し、結果を出力端子317に出力すると共に、シフタ402に供給する。

【0013】したがって、このLFSR902でも、関数発生回路202はレジスタ205からの現在の内部状態を表すデータを変換して出力し、レジスタ205は、

通常の動作状態においてクロック信号CLKの各クロックパルスが入力されるごとに、セレクタ204を通じて関数発生回路202が outputするデータを取り込んで保持する。したがって、各クロックが入力されるごとに内部状態が変化し、変化した内部状態にもとづいて関数発生回路202は擬似乱数を発生し、端子317から出力する。このようなLFSR902で、発生される擬似乱数の周期が $2^m - 1$ である場合には、このLFSRは特にM系列発生器と呼ばれる。

【0014】

【発明が解決しようとする課題】しかし、図7に示した従来の擬似乱数発生装置では、入力端子103からクロック信号が入力されても、クロック制御信号 Y_{j-1} が論理“1”の時には、上記クロックは論理和回路901で阻止され、したがって、LFSR902の内部状態は更新されない。その結果、上述したロックインの問題が発生し、ロックインを利用した暗号解読を防ぐべく、多数のLFSR902をカスケード接続しなければならなくなる。そのため、従来の擬似乱数発生装置は規模が大きく、かつコスト高となっていた。また、装置の規模およびコストに配慮して設計した場合には、性能が抑えられる結果となっていた。

【0015】そこで本発明の目的は、ロックインの問題を解決して小規模、低コストで、かつ暗号学的な安全性の高い擬似乱数を発生できる擬似乱数発生方法および装置を提供することにある。

【0016】

【課題を解決するための手段】本発明は上記目的を達成するため、順序づけられた複数の擬似乱数発生回路を用い、前段の前記擬似乱数発生回路が発生した第1の擬似乱数にもとづいて各擬似乱数発生回路に第1の擬似乱数を発生させ、前記複数の擬似乱数発生回路が発生した前記第1の擬似乱数により第2の擬似乱数を発生する擬似乱数発生方法において、各擬似乱数発生回路では、複数のビットから成る状態データを保持し、保持した前記状態データに応じて複数のビットから成る第1および第2のデータを発生し、前記第1および第2のデータのうちのいずれかのデータの特定のビットを、前段の前記擬似乱数発生回路が発生した前記第1の擬似乱数にもとづいて選択し前記第1の擬似乱数として出力し、前記第1および第2のデータのうちのいずれかのデータの、前記特定のビットを除いたデータを、前段の前記擬似乱数発生回路が発生した前記第1の擬似乱数にもとづいて選択し次に保持すべき前記状態データとすることを特徴とする。

【0017】本発明の擬似乱数発生方法はまた、保持した前記状態データに応じて複数のビットから成る順序づけられた複数のデータを発生し、前記複数のデータのうちの1番目のデータは前記状態データから直接発生し、2番目以降のデータはそれぞれ1つ前のデータから発生

し、前記第1のデータは前記複数のデータのうちの最後のデータを除くいずれかのデータであり、前記第2のデータは前記複数のデータのうちの最後のデータであることを特徴とする。本発明は擬似乱数発生方法また、 S_0, S_1 を $0 < S_0 < S_1$ を満たす整数として前記第1のデータは前記複数のデータのうちの S_0 番目のデータであって前記第2のデータは S_1 番目の前記データであり、 i を1以上の整数として i 番目の前記擬似乱数発生回路が発生する前記第1の擬似乱数の系列の周期を L_i とし、 i 番目の前記擬似乱数発生回路が発生する前記第1の擬似乱数の系列の1周期中に出現する論理“1”的数を W_i とし、任意の*i*に対して L_i と $(L_{i-1} - W_{i-1}) \times S_0 + W_{i-1} \times S_1$ とが互いに素で、2より大きい任意の*i*に対して L_i と $L_1 \times L_2 \times \cdots \times L_{i-2}$ とが互いに素であることを特徴とする。

【0018】また、本発明の擬似乱数発生装置は、順序づけられた複数の擬似乱数発生回路を備え、各擬似乱数発生回路は前段の前記擬似乱数発生回路が発生した第1の擬似乱数にもとづいて第1の擬似乱数を発生し、前記複数の前記擬似乱数発生回路が発生した前記第1の擬似乱数により第2の擬似乱数を発生する擬似乱数発生装置において、各擬似乱数発生回路は、複数のビットから成る状態データを、クロック信号の各クロックパルスに同期して取り込んで保持するレジスタと、前記レジスタが保持している前記状態データに応じて複数のビットから成る第1および第2のデータをそれぞれ出力する第1および第2の関数発生回路と、前記第1および第2の関数発生回路がそれぞれ出力する前記第1および第2のデータのうちのいずれかのデータの特定のビットを、前段の前記擬似乱数発生回路が発生した前記第1の擬似乱数にもとづいて選択し前記第1の擬似乱数として出力する第1のセレクタと、前記第1および第2の関数発生回路がそれぞれ出力する前記第1および第2のデータのうちのいずれかの前記データの、前記特定のビットを除いたデータを、前段の前記擬似乱数発生回路が発生した前記第1の擬似乱数にもとづいて選択し前記レジスタに前記状態データとして供給する第2のセレクタとを備えたことを特徴とする。

【0019】本発明の擬似乱数発生装置はまた、前記レジスタが保持している状態データに応じて複数のビットから成るデータをそれぞれ出力する順序づけられた複数の関数発生回路を含み、1番目の前記関数発生回路は前記レジスタが保持している前記状態データに直接したがって前記データを出し、2番目以降の前記関数発生回路はそれぞれ1つ前の前記関数発生回路が出したデータにしたがって前記データを出し、前記第1の関数発生回路は前記複数の関数発生回路のうちの最後の関数発生回路を除くいずれかの関数発生回路であり、第2の前記関数発生回路は前記複数の関数発生回路のうちの最後の関数発生回路であることを特徴とする。本発明の擬似

乱数発生装置はまた、 S_0, S_1 を $0 < S_0 < S_1$ を満たす整数として前記第1の関数発生回路は前記複数の関数発生回路のうちの S_0 番目の関数発生回路であって前記第2の関数発生回路は S_1 番目の関数発生回路であり、 i を1以上の整数として i 番目の前記擬似乱数発生回路が発生する前記第1の擬似乱数の系列の周期を L_i とし、 i 番目の前記擬似乱数発生回路が発生する前記第1の擬似乱数の系列の1周期中に出現する論理“1”的数を W_i とし、任意の*i*に対して L_i と $(L_{i-1} - W_{i-1}) \times S_0 + W_{i-1} \times S_1$ とが互いに素で、2より大きい任意の*i*に対して L_i と $L_1 \times L_2 \times \cdots \times L_{i-2}$ とが互いに素であるように、 S_0, S_1 および L_i が選定される。したがって、本発明では周期が最大の擬似乱数系列を発生することができる。

【0020】本発明の擬似乱数発生方法では、擬似乱数発生回路において複数のビットから成る状態データを保持し、保持した状態データに応じて複数のビットから成る第1および第2のデータを発生する。そして、第1および第2のデータのうちのいずれかのデータの特定のビットを、前段の擬似乱数発生回路が発生した第1の擬似乱数にもとづいて選択し第1の擬似乱数として出力する。一方、第1および第2のデータのうちのいずれかのデータの、上記特定のビットを除いたデータを、前段の擬似乱数発生回路が発生した第1の擬似乱数にもとづいて選択し次に保持すべき状態データとする。

【0021】また、本発明の擬似乱数発生装置では、擬似乱数発生回路において、レジスタは、複数のビットから成る状態データを、クロック信号の各クロックパルスに同期して取り込んで保持し、第1および第2の関数発生回路は、レジスタが保持している状態データに応じて複数のビットから成る第1および第2のデータをそれぞれ出力する。そして、第1のセレクタは、第1および第2の関数発生回路がそれぞれ出力する第1および第2のデータのうちのいずれかのデータの特定のビットを、前段の擬似乱数発生回路が発生した第1の擬似乱数にもとづいて選択し第1の擬似乱数として出力する。一方、第2のセレクタは、第1および第2の関数発生回路がそれぞれ出力する第1および第2のデータのうちのいずれかのデータの、上記特定のビットを除いたデータを、前段の擬似乱数発生回路が発生した第1の擬似乱数にもとづいて選択しレジスタに状態データとして供給する。したがって、本発明では、各擬似乱数発生回路の状態データが表す各擬似乱数発生回路の内部状態は前段が発生した擬似乱数に係わらず必ず変化し、そのためロックインの問題は発生しない。

【0022】また、本発明の擬似乱数発生方法および擬似乱数発生装置では、第1のデータまたは第1の関数発生回路は複数のデータまたは複数の関数発生回路のうちの S_0 番目のデータまたは関数発生回路であって第2のデータまたは第2の関数発生回路は S_1 番目のデータまたは関数発生回路であるとし、また、 i を1以上の整数として i 番目の擬似乱数発生回路が発生する第1の擬似

乱数の系列の周期を L_i 、 i 番目の擬似乱数発生回路が発生する第1の擬似乱数の系列の1周期中に出現する論理“1”的数を W_i とした場合、任意の*i*に対して L_i と $(L_{i-1} - W_{i-1}) \times S_0 + W_{i-1} \times S_1$ とが互いに素で、2より大きい任意の*i*に対して L_i と $L_1 \times L_2 \times \cdots \times L_{i-2}$ とが互いに素であるように、 S_0, S_1 および L_i が選定される。したがって、本発明では周期が最大の擬似乱数系列を発生することができる。

【0023】

10 【発明の実施の形態】次に本発明の実施の形態について図面を参照して説明する。図1は本発明による擬似乱数発生装置の一例の基本構成を示す機能ブロック図、図2は図1の擬似乱数発生装置を構成する擬似乱数発生回路を示す機能ブロック図である。以下ではこれらの図面を参照して本発明による擬似乱数発生装置の実施の形態について説明し、同時に本発明による擬似乱数発生方法の実施の形態について説明する。

【0024】図1に示したようにこの擬似乱数発生装置

100 100は、複数の擬似乱数発生回路101を備え、擬似乱数発生回路101には、入力端子103を通じてクロック信号CLKが入力され、入力端子104からは制御信号Lが入力されている。また、入力端子105からは各擬似乱数発生回路101が最初に保持するmビットのデータ（各擬似乱数発生回路101ごとに異なる）が入力される。 i 番目（ n を正の整数として $i = 1, 2, \dots, n$ ）の擬似乱数発生回路101が発生した擬似乱数 X_i （本発明に係わる第1の擬似乱数）は次段（ $i+1$ 番目）の擬似乱数発生回路101に状態制御信号として入力される。ただし、最初の擬似乱数発生回路

30 101には、論理値が一定（本実施の形態では論理“0”）の状態制御信号（ X_0 ）が入力されている。排他的論理和回路102は、すべての擬似乱数発生回路101が発生した擬似乱数 $X_{1 \sim n}$ の排他的論理和を計算し、計算結果をこの擬似乱数発生装置100が発生した擬似乱数（本発明に係わる第2の擬似乱数）として出力端子106を通じて出力する。

【0025】擬似乱数発生回路101は、後に詳しく説明するように内部状態をスキップする機能を有し、具体的には図2に示したように、レジスタ205、関数発生回路2021、2022、セレクタ203、206により構成されている。レジスタ205は、入力端子215からクロック信号CLKの各クロックパルスが供給されるごとに、セレクタ206が出力しているmビットのデータを内部状態を表すデータ（本発明に係わる状態データ）として取り込んで保持し、同時に、保持したデータを関数発生回路2021に出力する。

40 【0026】関数発生回路2021は、レジスタ205から供給されるmビットのデータに対して予め決められた変換を施し、もとのデータより1ビット多い $m+1$ ビットのデータを発生し、発生したデータの各ビットのう

ちmビットを関数発生回路2022とセレクタ206とに供給し、一方、残りの1ビット（本発明に係わる特定のビット）をセレクタ203に供給する。関数発生回路2022は関数発生回路2021と同様に構成され、関数発生回路2021から供給されるmビットのデータに対して予め決められた変換を施して、m+1ビットのデータを発生し、発生したデータの各ビットのうちmビットをセレクタ206に供給し、一方、残りの1ビットをセレクタ203に供給する。なお、関数発生回路2022は関数発生回路2021からのデータにもとづいて新たなデータを発生するので、結局レジスタ205が保持しているデータに応じて新たなデータを発生していることになる。

【0027】セレクタ206は、入力端子214から供給される制御信号Lが論理“0”の時は、入力端子213から供給されるmビットのデータP_I_iを選択して出力する。一方、入力端子214から供給される制御信号Lが論理“1”的時は、入力端子216から供給される前段（i-1番目）の擬似乱数発生回路101からの擬似乱数X_{i-1}（状態制御信号）が論理“0”であれば関数発生回路2021の出力データを選択して出力し、入力端子216から供給される擬似乱数X_{i-1}が論理“1”であれば関数発生回路2022の出力データを選択して出力する。

【0028】また、セレクタ203は、入力端子216から供給される擬似乱数X_{i-1}が論理“0”であれば、関数発生回路2021の出力を選択して出力し、入力端子216から供給される擬似乱数X_{i-1}が論理“1”であれば、関数発生回路2022の出力を選択して出力する。そして、このセレクタ203の出力が、i番目の擬似乱数発生回路101が発生した擬似乱数X_iとして出力端子217より出力される。

【0029】この擬似乱数発生回路101では、まず最初に論理“0”的制御信号Lが入力され、入力端子213から供給されるデータP_I_iがセレクタ206を通じてレジスタ205に入力され、入力端子215からクロック信号CLKのクロックパルスが入力されると、レジスタはこのデータP_I_iを最初の状態データとして取り込んで保持する。その後、制御信号Lは論理“1”に設定され、以降、セレクタ203、206は前段の擬似乱数発生回路101が発生した擬似乱数発生回路X_{i-1}の論理値にしたがって、関数発生回路2021、2022のいずれかがOutputした1ビットおよびmビットのデータを選択してそれぞれ出力端子217およびレジスタ205に出力する。

【0030】このように、レジスタ205が保持したデータは、関数発生回路2021、2024で変換され、いずれかの関数発生回路2021、2024のデータがセレクタ206を通じてレジスタ205に入力される。そして、レジスタ205はクロック信号CLKの各クロ

ックパルスごとに、入力されたデータを新たな状態を表すデータとして取り込み、保持する。そのため、この擬似乱数発生回路101では、前段の擬似乱数発生回路101が発生した擬似乱数X_{i-1}の論理値に係わらず、クロック信号CLKの各クロックパルスが入力されるごとにレジスタ205は必ず新たなデータを取り込んで保持し、したがって、各クロックパルスごとに必ず内部状態が変化する。そして、このような内部状態の変化に応じて擬似乱数X_iがOutput端子217から出力される。

【0031】なお、セレクタ206は、入力端子216から供給される前段の擬似乱数発生回路101からの擬似乱数X_{i-1}（状態制御信号）が論理“1”であれば関数発生回路2022の出力を選択して出力するので、擬似乱数X_{i-1}が論理“1”的ときは、本来次の内部状態を表すデータとして関数発生回路2021が出力しているデータはスキップされ、関数発生回路2022の出力データがレジスタ205に保持される。

【0032】次に、このように構成された擬似乱数発生装置100の動作について説明する。図1の擬似乱数発生装置100に擬似乱数を発生させるには次のようにする。まず、各擬似乱数発生回路101の内部状態を初期化するため、各擬似乱数発生回路101ごとに異なるmビットのデータを入力端子105に供給し、そして、入力端子104に論理“0”的制御信号Lを供給して入力端子103からはクロック信号CLKを供給する。その結果、各擬似乱数発生回路101内の上記レジスタ205（図2）に入力端子105から供給したmビットのデータがセレクタ206を通じてレジスタ205に入力され、保持される。

【0033】次に、入力端子104に論理“1”的制御信号Lを供給し、入力端子103からはクロック信号CLKを供給して通常の動作状態とする。これにより、各擬似乱数発生回路101では、入力端子103から供給したクロック信号の各クロックパルスがレジスタ205に入力されるごとに、レジスタ205は、上述のようにして関数発生回路2021、2022が発生した新たな状態を表すデータをセレクタ206を通じて取り込み、保持する。その際、セレクタ206は、前段の擬似乱数発生回路101が発生した擬似乱数X_{i-1}（状態制御信号）の論理値にしたがって関数発生回路2021、2022のいずれかが発生したデータを選択してレジスタ205に供給する。

【0034】そのため、各擬似乱数発生回路101では、前段の擬似乱数発生回路101が発生した擬似乱数X_{i-1}の論理値が論理“0”あるいは論理“1”的いずれであっても、クロック信号CLKの各クロックパルスが入力されるごとにレジスタ205は必ず新たなデータを取り込んで保持し、したがって、各クロックパルスごとに必ず内部状態が変化する。

【0035】そして、各擬似乱数発生回路101の関数

発生回路2021、2022はこの内部状態に応じて決る1ビットのデータを発生してセレクタ203に出力し、セレクタ203は前段の擬似乱数発生回路101が発生した擬似乱数 X_{i-1} の論理値にもとづいて関数発生回路2021、2022からの上記1ビットのデータのいずれかを選択し、出力端子217から擬似乱数 X_i として出力する。排他的論理和回路102は、すべての擬似乱数発生回路101が発生した擬似乱数 X_{1-n} の排他的論理和を計算し、計算結果をこの擬似乱数発生装置100が発生した擬似乱数として出力端子106を通じて出力する。

【0036】このように本実施の形態の擬似乱数発生装置100では、各擬似乱数発生回路101の内部状態は前段が発生した擬似乱数（状態制御信号）の論理値に係わらず必ず変化するので、ロックインの問題は発生しない。したがって、この擬似乱数発生装置100では暗号学的に高い安全性を備えた擬似乱数を発生することができる。また、多数の擬似乱数発生回路101を用いなくとも安全性の高い擬似乱数を発生することができるので、装置の小型化および低コスト化を図ることが可能である。

【0037】なお、この擬似乱数発生装置100では各擬似乱数発生回路101において2つの関数発生回路を用いたが、図3に示したようにさらに多くの関数発生回路を配列することも可能である。この擬似乱数発生回路110では、 S_0 、 S_1 を $0 < S_0 < S_1$ を満たす整数として、レジスタ205の保持データが入力される最初の関数発生回路2020から数えて S_0 番目の関数発生回路2021および S_1 番目（最後）の関数発生回路2022の出力データ（ $m+1$ ビット）がセレクタ203、206に供給されている。

【0038】この擬似乱数発生回路110でも、上述した擬似乱数発生回路101の場合と同様に、前段の擬似乱数発生回路が発生した擬似乱数 X_{i-1} の論理値に係わらず、クロック信号CLKの各クロックパルスが入力されることにレジスタ205は必ず新たなデータを取り込んで保持し、したがって、各クロックごとに必ず内部状態が変化する。そして、このような内部状態の変化に応じて擬似乱数 X_i が出力端子217から出力される。そのため、擬似乱数発生回路110を用いた場合にもロックインを起すことなく擬似乱数を発生することができる。

【0039】ただし、擬似乱数発生回路110ではより多くの関数発生回路が必要であるから、装置の規模およびコストの点では不利となる。したがって、2つの関数発生回路を用いた擬似乱数発生回路101は、装置の小型化と、擬似乱数の暗号学的な安全性を両立できるという点では最適である。なお、擬似乱数発生回路110において $S_0=1$ 、 $S_1=2$ とすると擬似乱数発生回路110は上述した擬似乱数発生回路101と同一構成とな

る。

【0040】本実施の形態の擬似乱数発生装置100では、各擬似乱数発生回路101のレジスタ205が保持する内部状態を表すデータはすべて m ビットで同一であるとしたが、本発明では従来と異なり、このビット数を各擬似乱数発生回路101ごとに異なる値とすることも可能である。そのような構成とした場合にも、各擬似乱数発生回路101は上述の場合と基本的に同様に動作してそれぞれ擬似乱数を発生し、排他的論理和回路102が各擬似乱数発生回路101が発生した擬似乱数の排他的論理和を算出することで最終的な擬似乱数が得られる。そして、内部状態を表すデータのビット数を擬似乱数発生回路ごとに変えることで多様性が増し、発生される擬似乱数はより質が向上して暗号学的な安全性は一層高まる。

【0041】さらにパラメータを次のように最適化することにより擬似乱数発生装置100の性能を一層高めることができる。ここでは、一般化のため擬似乱数発生装置100は上記擬似乱数発生回路110で構成され、また内部状態を表すデータのビット数は擬似乱数発生回路ごとに任意に設定されているものとする。そして、 i 番目の擬似乱数発生回路110が発生する擬似乱数系列の周期を L_i とし、 i 番目の擬似乱数発生回路110が発生する擬似乱数系列の1周期中に出現する論理“1”的数を W_i として、任意の i に対して L_i と $(L_{i-1}-W_{i-1}) \times S_0 + W_{i-1} \times S_1$ が互いに素で、2より大きい任意の i に対して L_i と $L_1 \times L_2 \times \dots \times L_{i-2}$ が互いに素となるように、 S_0 、 S_1 および周期 L_i を選定する。なお、擬似乱数発生装置100を図1のように擬似乱数発生回路101で構成した場合は、 S_0 、 S_1 は $S_0=1$ 、 $S_1=1$ に選定されているので、残る周期 L_i を上記条件を満たすように選定することになる。 S_0 、 S_1 および周期 L_i をこのように選定することで、擬似乱数発生装置100が输出する擬似乱数系列の周期を最大にすることができる。

【0042】このことは、次のようにして証明できる。まず、図1において、擬似乱数 X_{i-1} の周期が $L_1 \times L_2 \times \dots \times L_{i-1}$ で、その1周期中に出現する論理“0”的数と論理“1”的数との比が $(L_{i-1}-W_{i-1}) : W_{i-1}$ であると仮定する。このとき、 i 番目の擬似乱数発生回路110（101）の内部状態は、 $L_1 \times L_2 \times \dots \times L_{i-1}$ 時間の後に、ちょうど $\{(L_{i-1}-W_{i-1}) \times S_0 + W_{i-1}S_1\} \times L_1 \times L_2 \times \dots \times L_{i-2}$ クロックパルス分だけ更新される。

【0043】ところで、上述のように、任意の i に対して L_i と $(L_{i-1}-W_{i-1}) \times S_0 + W_{i-1} \times S_1$ が互いに素で、2より大きい任意の i に対して L_i と $L_1 \times L_2 \times \dots \times L_{i-2}$ が互いに素となるように、 S_0 、 S_1 および周期 L_i を選定すると、擬似乱数 X_{i-1} と i 番目の擬似乱数発生回路110（101）の内部状態の両方が同時に

ちょうど一巡するのは、 $L_1 \times L_2 \times \dots \times L_{i-1} \times L_i$ 時間の後であるから、擬似乱数 X_i の周期は $L_1 \times L_2 \times \dots \times L_{i-1} \times L_i$ で、その間に i 番目の擬似乱数発生回路 110 (101) のどの内部状態も等しい回数だけスキップされている。したがって、擬似乱数 X_i の 1 周期中に出現する論理 "0" と論理 "1" の数の比は $(L_{i-1} - W_{i-1}) : W_{i-1}$ となる。ところで、この仮定は、 $i = 2$ の場合には成り立っているから、以上の議論は、 $i = 2$ から出発して、 $i = 2, 3, \dots, n$ についてまで適用できる。従って、擬似乱数 X_n の周期（すなわち擬似乱数発生装置 100 が発生する擬似乱数の周期）は $L_1 \times L_2 \times \dots \times L_n$ となる。そして、この周期は、それぞれの周期が L_i である擬似乱数発生回路を組み合わせて得られる擬似乱数の周期の最大値に等しい。したがって、本実施の形態の擬似乱数発生装置 100 では、上記条件を満たすように S_0, S_1 、および周期 L_i を選定することで、擬似乱数発生装置 100 が output する擬似乱数系列の周期を最大にすることができる。

【0044】なお、図 3 の擬似乱数発生回路で $S_0 = 0, S_1 = 1$ と選ぶと、擬似乱数発生回路 110 は図 8 に示した擬似乱数発生回路と同一構成となり、その場合、擬似乱数発生回路 110 の内部状態は、 $L_1 \times L_2 \times \dots \times L_{i-1}$ 時間の後に、 $W_{i-1} \times L_1 \times L_2 \times \dots \times L_{i-2}$ クロックパルス分だけ更新されることになるが、図 7 に示した従来の擬似乱数発生装置では内部状態が常に更新されるとは限らないので、ちょうど $W_{i-1} \times L_1 \times L_2 \times \dots \times L_{i-2}$ クロックパルス分だけ常に更新されるとは言えず、以上の議論は適用できない。

【0045】なお、擬似乱数発生装置 100 では排他的論理和回路 102 により、各擬似乱数発生回路 101 が発生した擬似乱数の排他的論理和を算出して擬似乱数を得ているが、各擬似乱数発生回路 101 が発生した擬似乱数に対して排他的論理和以外の演算を行って擬似乱数を発生することも可能である。ただし、排他的論理和を使うことが、擬似乱数の暗号学的な安全性と装置の小規模化を両立できるという点で最適である。

【0046】また、排他的論理和回路 102 の代りに各擬似乱数発生回路 101 ごとに排他的論理和回路を設ける構成とすることも可能である。図 4 は、各擬似乱数発生回路ごとに排他的論理和回路を設けた場合の発明の実施の形態を示す機能ブロック図である。この擬似乱数発生装置 111 では、各擬似乱数発生回路 101 ごとに排他的論理和回路 802 が設けられ、 i 番目の排他的論理和 802 の一方の入力端子には $i - 1$ 番目の排他的論理和回路 802 が output する擬似乱数 Y_{i-1} が入力され、もう一方の入力端子には i 番目の擬似乱数発生回路 101 が発生した擬似乱数 X_i が入力されている。そして、 $i - 1$ 番目の排他的論理和回路 802 からの擬似乱数 Y_{i-1} が状態制御信号として i 番目の擬似乱数発生回路 101 に供給されている。また、最後の排他的論理和回路

802 が算出した擬似乱数 Y_n がこの擬似乱数発生装置 111 が発生した擬似乱数として出力端子 106 より出力されている。

【0047】このような構成においても擬似乱数 X_i と擬似乱数 Y_i との性質は等しいので、擬似乱数発生装置 111 は擬似乱数発生装置 100 と同様に動作し、したがって擬似乱数発生装置 100 と同様の効果が得られる。そして、この擬似乱数発生装置 111 では、擬似乱数発生回路 101 と排他的論理和 802 を 1 つの集積回路に搭載することができ、それらをカスケード接続することによって所望の安全性を持つ擬似乱数発生装置を簡単に構成できる。

【0048】図 1 の擬似乱数発生装置 100 を構成する擬似乱数発生回路 101 は、図 8 に示した従来の擬似乱数発生回路において、関数発生回路を複数にして上述のような内部状態のスキップ機能を持たせたものである。したがって、図 9 に示した非線形フィードバック・シフトレジスタでも、この非線形フィードバック・シフトレジスタの基本構成は図 8 の擬似乱数発生回路と同じであるから、同様にして容易にスキップ機能を持たせ、図 1 の擬似乱数発生装置 100 において、擬似乱数発生回路 101 の代りに用いることができる。そして、図 8 の非線形フィードバック・シフトレジスタにスキップ機能を持たせて利用した場合には、関数発生回路の構成が簡素となるので装置の小型化に有効である。

【0049】また、図 9 に示した LFSR でも同様にして容易に内部状態のスキップ機能を持たせることができ、擬似乱数発生回路 101 の代りに用いることができる。この場合にも関数発生回路の構成が簡素となるので装置の小型化に有効である。

【0050】なお、図 2 に示した擬似乱数発生回路 101 において、セレクタ 206 に供給される m ビットのデータ、したがってまたレジスタ 205 に供給される m ビットのデータはシリアルデータおよびパラレルデータのいずれであってもかまわない。そして、内部状態を表すデータのビット数が擬似乱数発生回路 101 ごとに異なる場合、 $1 \sim n$ (n は 2 以上の整数) の各擬似乱数発生回路 101 に対して最初にそれぞれ m_1, m_2, \dots, m_n ビットのデータを供給するとき、これらのデータを $m_1 + m_2 + \dots + m_n$ ビットのビット列として入力端子 213 に供給し、各擬似乱数発生回路 101 のレジスタ 205 には対応するビット列部分をそれぞれ保持させることも可能である。

【0051】次に本発明の第 2 の実施の形態について説明する。図 5 は、第 2 の実施の形態の擬似乱数発生装置の基本構成を示す機能ブロック図、図 6 は図 5 の擬似乱数発生装置を構成する擬似乱数発生回路を示す機能ブロック図である。図中、図 1、図 2 と同一の要素には同一の符号が付されており、それらに関する詳しい説明はここでは省略する。

【0052】この擬似乱数発生装置112が、擬似乱数発生装置100と機能的に異なるのは複数ビットのデータとして擬似乱数を発生する点であり、一方、構成の点では、擬似乱数発生回路601の構成が異なり、また関数発生回路603が追加されている点で異なっている。図5に示したようにこの擬似乱数発生装置112は、多値の擬似乱数を発生する複数の擬似乱数発生回路601を備え、擬似乱数発生回路601には、入力端子103を通じてクロック信号CLKが入力され、入力端子104からは制御信号Lが入力されている。また、入力端子105からは擬似乱数発生回路601が最初に保持するmビットのデータが入力される。

【0053】i番目(nを正の整数としてi=1, 2, ..., n)の擬似乱数発生回路601が発生した擬似乱数 X_i (kを2以上の整数としてkビットのデータ)は、各擬似乱数発生回路601ごとに設けられた関数発生回路603に入力され、関数発生回路603はこの擬似乱数 X_i に予め決められた変換を施して1ビットのデータとし、擬似乱数 Z_i (状態制御信号)として次段(i+1番目)の擬似乱数発生回路601に出力する。ただし、最初の擬似乱数発生回路601には、論理値が一定(本実施の形態では論理"0")の状態制御信号(Z_0)が入力されている。排他的論理和回路602は、すべての擬似乱数発生回路601が発生した擬似乱数 $X_{1~n}$ のkビットのデータとしての排他的論理和を計算し、計算結果をこの擬似乱数発生装置112が発生したkビットの擬似乱数として出力端子106を通じて出力する。

【0054】i番目の擬似乱数発生回路601は図6に示したように、レジスタ205、関数7021、7022、セレクタ703、206により構成されている。レジスタ205は、入力端子215からクロック信号CLKの1つのクロックパルスが供給されるごとに、セレクタ206が出力しているmビットのデータを内部状態を表すデータ(本発明に係わる状態データ)として保持し、同時に、保持したデータを関数発生回路7021に出力する。

【0055】関数発生回路7021は、レジスタ205から供給されるmビットのデータに対して予め決められた変換を施し、もとのデータよりkビット多いm+kビットのデータを発生し、発生したデータの各ビットのうちmビットを関数発生回路7022とセレクタ206とに供給し、一方、残りのkビット(本発明に係わる特定のビット)をセレクタ703に供給する。関数発生回路7022は関数発生回路7021と同様に構成され、関数発生回路7021から供給されるmビットのデータに対して予め決められた変換を施して、m+kビットのデータを発生し、発生したデータの各ビットのうちmビットをセレクタ206に供給し、一方、残りのkビットをセレクタ703に供給する。なお、関数発生回路702

2は関数発生回路7021からのデータにもとづいて新たなデータを発生するので、結局レジスタ205が保持しているデータに応じて新たなデータを発生していることになる。

【0056】セレクタ703は、入力端子216から供給される前段からの擬似乱数 Z_{i-1} (状態制御信号)が論理"0"であれば、関数発生回路7021の出力を選択して出力し、入力端子216から供給される状態制御信号 Z_{i-1} が論理"1"であれば、関数発生回路7022の出力を選択して出力する。そして、このセレクタ703の出力が、擬似乱数発生回路601が発生したkビットの擬似乱数 X_i として出力端子717より出力される。

【0057】この擬似乱数発生回路601でも、セレクタ206は、入力端子216から供給される前段の擬似乱数発生回路601からの状態制御信号 Z_{i-1} が論理"1"であれば関数発生回路7022の出力を選択して出力するので、状態制御信号 Z_{i-1} が論理"1"のときは、本来次の内部状態を表すデータとして関数発生回路7021が出力しているデータはスキップされ、関数発生回路7022の出力データがレジスタ205に保持される。

【0058】この擬似乱数発生回路601では、まず最初に論理"0"の制御信号Lが入力され、入力端子213から供給されるデータ P_I_i がセレクタ206を通じてレジスタ205に入力され、入力端子215からクロック信号CLKのクロックパルスが入力されると、レジスタはこのデータ P_I_i を最初の状態データとして取り込んで保持する。その後、制御信号Lは論理"1"に設定され、以降、セレクタ703、206は前段の関数発生回路603が発生した擬似乱数 Z_{i-1} の論理値にしたがって、関数発生回路7021、7022のいずれかが出力したkビットおよびmビットのデータを選択してそれぞれ出力端子717およびレジスタ205に出力する。

【0059】このように、レジスタ205が保持したデータは、関数発生回路7021、7022で変換され、いずれかの関数発生回路7021、7022のデータがセレクタ206を通じてレジスタ205に入力される。そして、レジスタ205はクロック信号CLKの各クロックパルスごとに、入力されたデータを新たな状態を表すデータとして取り込み、保持する。

【0060】そのため、この擬似乱数発生回路601では、前段の関数発生回路603が発生した擬似乱数 Z_{i-1} の論理値に係わらず、クロック信号CLKの各クロックパルスが入力されるごとにレジスタ205は必ず新たなデータを取り込んで保持し、したがって、各クロックごとに必ず内部状態が変化する。そして、このような内部状態の変化に応じてkビットの擬似乱数 X_i が出力端子217から出力される。

【0061】次に、このように構成された擬似乱数発生

装置112の動作について説明する。図5の擬似乱数発生装置112に擬似乱数を発生させるには次のようにする。まず、各擬似乱数発生回路601の内部状態を初期化するためのmビットのデータ（擬似乱数発生回路601ごとに異なる）を入力端子105に供給し、そして、入力端子104に論理“0”的制御信号Lを供給して入力端子103からはクロック信号CLKを入力する。その結果、各擬似乱数発生回路601内の上記レジスタ205（図6）に入力端子105から供給したmビットのデータがセレクタ206を通じてレジスタ205に入力され、保持される。

【0062】次に、入力端子104に論理“1”的制御信号Lを供給し、入力端子103からはクロック信号CLKを供給して通常の動作状態とする。これにより、各擬似乱数発生回路601では、入力端子103から供給したクロック信号の各クロックパルスがレジスタ205に入力されるごとに、レジスタ205は、上述のようにして関数発生回路7021、7022が発生した新たな状態を表すデータをセレクタ206を通じて取り込み、保持する。その際、セレクタ206は、前段の擬似乱数発生回路601が発生した擬似乱数 X_{i-1} を関数発生回路603が変換して発生した擬似乱数 Z_{i-1} （状態制御信号）の論理値にしたがって関数発生回路7021、7022のいずれかが発生したデータを選択してレジスタ205に供給する。

【0063】そのため、各擬似乱数発生回路601では、前段の擬似乱数発生回路601に対応する関数発生回路603が発生した擬似乱数 Z_{i-1} （状態制御信号）の論理値が論理“0”あるいは論理“1”的いずれであっても、クロック信号CLKの各クロックパルスが入力されるごとにレジスタ205は必ず新たなデータを取り込んで保持し、したがって、各クロックごとに必ず内部状態が変化する。

【0064】そして、各擬似乱数発生回路601の関数発生回路7021、7022はこの内部状態に応じて決るkビットのデータを発生してセレクタ703に出力し、セレクタ703は前段の擬似乱数発生回路601に対応する関数発生回路603が発生した擬似乱数 Z_{i-1} （状態制御信号）の論理値にもとづいて関数発生回路7021、7022からの上記kビットのデータのいずれかを選択し、出力端子717からkビットの擬似乱数 X_i として出力する。排他的論理和回路602は、すべての擬似乱数発生回路601が発生した擬似乱数 X_{1-n} の排他的論理和を計算し、計算結果をkビットの擬似乱数として出力端子606を通じて出力する。

【0065】したがってこの擬似乱数発生装置112でも、各擬似乱数発生回路601の内部状態は前段が発生した擬似乱数にもとづく状態制御信号の論理値に係わらず必ず変化するので、ロックインの問題は発生しない。そのため、擬似乱数発生装置112では暗号学的に高い

安全性を備えた擬似乱数を発生することができる。また、多数の擬似乱数発生回路601を用いなくとも安全性の高い擬似乱数を発生することができるので、装置の小型化および低コスト化を図ることが可能である。なお、この擬似乱数発生装置112では各擬似乱数発生回路601において2つの関数発生回路を用いたが、擬似乱数発生装置100の場合と同様、擬似乱数発生回路110（図3）のようにさらに多くの関数発生回路を配列することも可能である。ただし、そのような構成ではより多くの関数発生回路が必要であるから、装置の規模およびコストの点では不利となる。したがって、2つの関数発生回路を用いた擬似乱数発生回路601は、装置の小型化と、擬似乱数の暗号学的な安全性を両立できるという点では最適である。

【0066】また、この擬似乱数発生装置112では、各擬似乱数発生回路601のレジスタ205が保持する内部状態を表すデータはすべてmビットで同一であるとしたが、擬似乱数発生装置100の場合と同様に、このビット数を各擬似乱数発生回路601ごとに異なる値とすることも可能である。そのような構成とした場合にも、各擬似乱数発生回路601は上述の場合と基本的に同様に動作してそれぞれ擬似乱数を発生し、排他的論理和回路602が各擬似乱数発生回路601が発生した擬似乱数の排他的論理和を算出することで擬似乱数が得られる。そして、内部状態を表すデータのビット数を擬似乱数発生回路ごとに変えることで多様性が増し、発生される擬似乱数はより質が向上して暗号学的な安全性は一層高まる。

【0067】さらに、この擬似乱数発生装置112においてもパラメータを最適化することにより性能を一層高めることができる。すなわち、i番目の擬似乱数発生回路601が発生する擬似乱数系列の周期を L_i とし、i番目の関数発生回路603が outputする状態制御信号 Z_i （擬似乱数系列）の1周期中に出現する論理“1”的数を W_i として、任意のiに対して L_i と $(L_{i-1}-W_{i-1}) \times S_0 + W_{i-1} \times S_1$ とが互いに素で、2より大きい任意のiに対して L_i と $L_1 \times L_2 \times \dots \times L_{i-2}$ とが互いに素となるように、 S_0 、 S_1 および周期 L_i を選定する。

【0068】なお、一般化のため擬似乱数発生回路601において内部状態を表すデータのビット数は擬似乱数発生回路601ごとに任意に設定されているものとする。また、 S_0 、 S_1 は、擬似乱数発生回路110の場合と同様、擬似乱数発生回路601において関数発生回路をさらに多数配列した場合に、何番目の関数発生回路からセレクタ206にデータが供給されているかを表す数であり、 S_0 番目と S_1 番目の関数発生回路からセレクタ206にデータが供給され、 S_1 番目の関数発生回路が最後の関数発生回路である。 S_0 、 S_1 および周期 L_i を上記条件を満たすように選定することで、擬似乱数発生装置112が出力する擬似乱数系列の周期を最大にする

ことができる。このことは、擬似乱数発生装置100の場合と同様にして証明できるので、ここではその証明は省略する。なお、擬似乱数発生装置112では $S_0=1$ 、 $S_1=2$ であるから、擬似乱数発生装置112の場合は上記条件を満たすように周期 L_i を選定することになる。

【0069】擬似乱数発生装置112では排他的論理和回路602により、各擬似乱数発生回路601が発生した擬似乱数の排他的論理和を算出して擬似乱数を得ているが、各擬似乱数発生回路601が発生した擬似乱数に対して排他的論理和以外の演算を行って擬似乱数を発生することも可能である。ただし、排他的論理和を使うことが、擬似乱数の暗号学的な安全性と装置の小規模化を両立できるという点で最適である。また、擬似乱数発生装置111(図4)のように、排他的論理和回路602の代りに各擬似乱数発生回路601ごとに排他的論理和回路を設ける構成とすることも可能である。

【0070】

【発明の効果】以上説明したように本発明の擬似乱数発生方法では、擬似乱数発生回路において複数のビットから成る状態データを保持し、保持した状態データに応じて複数のビットから成る第1および第2のデータを発生する。そして、第1および第2のデータのうちのいずれかのデータの特定のビットを、前段の擬似乱数発生回路が発生した第1の擬似乱数にもとづいて選択し第1の擬似乱数として出力する。一方、第1および第2のデータのうちのいずれかのデータの、上記特定のビットを除いたデータを、前段の擬似乱数発生回路が発生した第1の擬似乱数にもとづいて選択し次に保持すべき状態データとする。

【0071】また、本発明の擬似乱数発生装置では、擬似乱数発生回路において、レジスタは、複数のビットから成る状態データを、クロック信号の各クロックパルスに同期して取り込んで保持し、第1および第2の関数発生回路は、レジスタが保持している状態データに応じて複数のビットから成る第1および第2のデータをそれぞれ出力する。そして、第1のセレクタは、第1および第2の関数発生回路がそれぞれ出力する第1および第2のデータのうちのいずれかのデータの特定のビットを、前段の擬似乱数発生回路が発生した第1の擬似乱数にもとづいて選択し第1の擬似乱数として出力する。一方、第2のセレクタは、第1および第2の関数発生回路がそれ出力する第1および第2のデータのうちのいずれかのデータの、上記特定のビットを除いたデータを、前段の擬似乱数発生回路が発生した第1の擬似乱数にもとづいて選択しレジスタに状態データとして供給する。

【0072】したがって、本発明では、各擬似乱数発生回路の状態データが表す各擬似乱数発生回路の内部状態は前段が発生した擬似乱数に係わらず必ず変化し、そのためロックインの問題は発生しない。その結果、本発明

では暗号学的に高い安全性を備えた擬似乱数を発生できる。また、ロックインの問題がないので多数の擬似乱数発生回路を用いなくとも安全性の高い擬似乱数を発生することができ、装置の小型化および低コスト化を図ることが可能である。そして、本発明では状態データのビット数を擬似乱数発生回路ごとに変えることが可能であるから、多様性を増大させて、発生される擬似乱数の質を一層向上させ、暗号学的な安全性を一層高めることができる。さらに、擬似乱数を複数のビットから成るデータとして発生する多値の擬似乱数発生回路を用いることができる、より利用範囲を拡大することができる。

【0073】また、本発明の擬似乱数発生方法および擬似乱数発生装置では、第1のデータまたは第1の関数発生回路は複数のデータまたは複数の関数発生回路のうちの S_0 番目のデータまたは関数発生回路であって第2のデータまたは第2の関数発生回路は S_1 番目のデータまたは関数発生回路であるとし、また、 i を1以上の整数として i 番目の擬似乱数発生回路が発生する第1の擬似乱数の系列の周期を L_i 、 i 番目の擬似乱数発生回路が発生する第1の擬似乱数の系列の1周期中に出現する論理“1”的数を W_i とした場合、任意の i に対して L_i と $(L_{i-1}-W_{i-1}) \times S_0 + W_{i-1} \times S_1$ とが互いに素で、2より大きい任意の i に対して L_i と $L_1 \times L_2 \times \dots \times L_{i-2}$ とが互いに素であるように、 S_0 、 S_1 および L_i が選定される。したがって、本発明では周期が最大の擬似乱数系列を発生することができる。

【図面の簡単な説明】

【図1】本発明による擬似乱数発生装置の一例の基本構成を示す機能ブロック図である。

【図2】図1の擬似乱数発生装置を構成する擬似乱数発生回路を示す機能ブロック図である。

【図3】より多くの関数発生回路を用いた擬似乱数発生回路を示す機能ブロック図である。

【図4】各擬似乱数発生回路ごとに排他的論理和回路を設けた場合の発明の実施の形態を示す機能ブロック図である。

【図5】第2の実施の形態の擬似乱数発生装置の基本構成を示す機能ブロック図である。

【図6】図5の擬似乱数発生装置を構成する擬似乱数発生回路を示す機能ブロック図である。

【図7】線形フィードバック・シフトレジスタ(LFSR)をカスケード接続した従来の擬似乱数発生装置の基本構成を示す機能ブロック図である。

【図8】従来の基本的な構成の擬似乱数発生回路の一例を示す機能ブロック図である。

【図9】非線形フィードバック・シフトレジスタと呼ばれる従来の擬似乱数発生回路の基本構成を示す機能ブロック図である。

【図10】図7の擬似乱数発生装置を構成する線形フィードバック・シフトレジスタの基本構成を示す機能ブロ

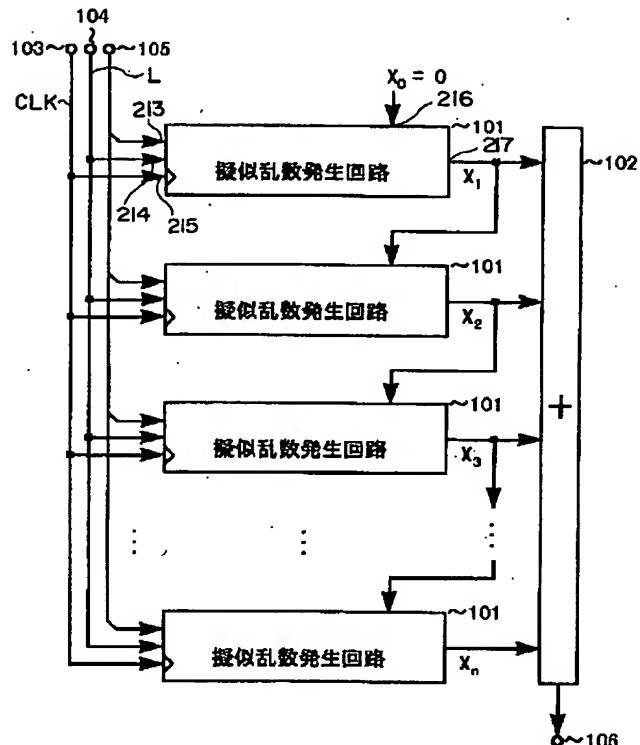
ック図である。

【符号の説明】

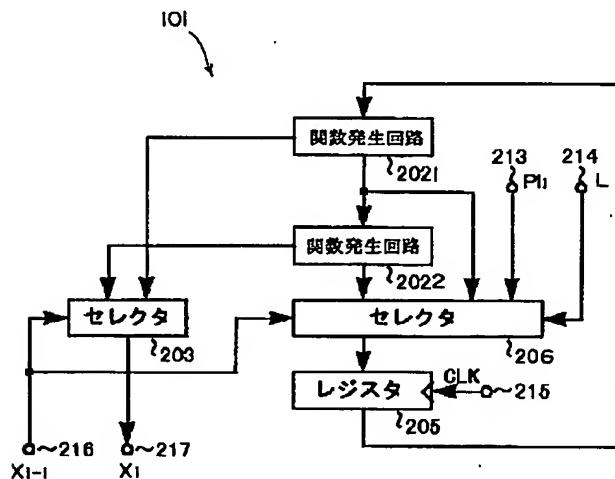
100、111、112……擬似乱数発生装置、101、110、601……擬似乱数発生回路、102、6

02、802……排他的論理和回路、205……レジスタ、203、206、703……セレクタ、603、2021、2020、2022、7021、7022……関数発生回路。

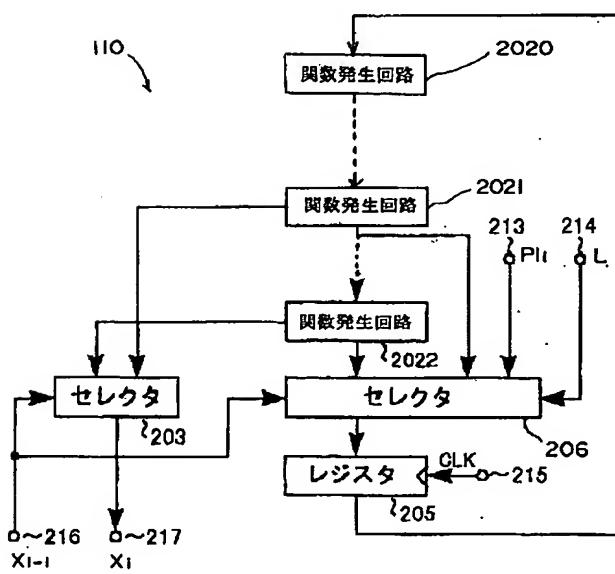
【図1】



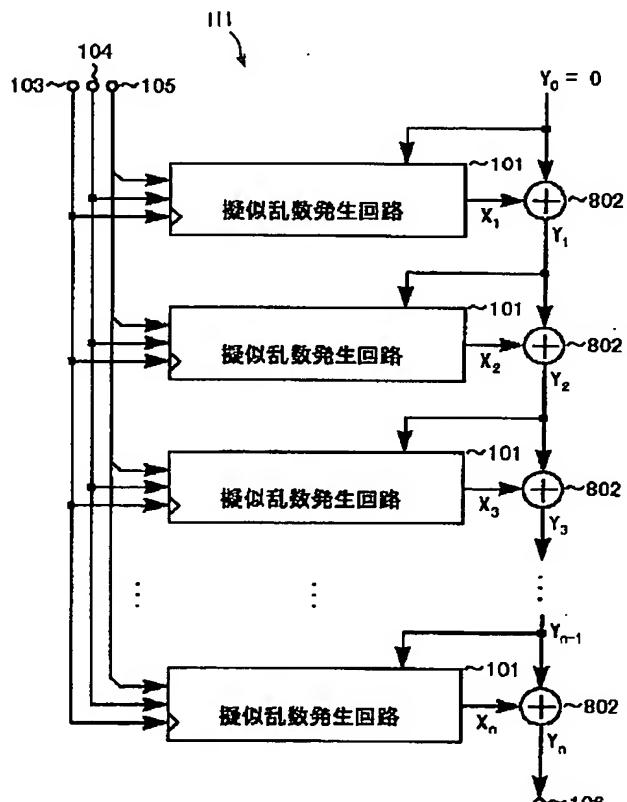
【図2】



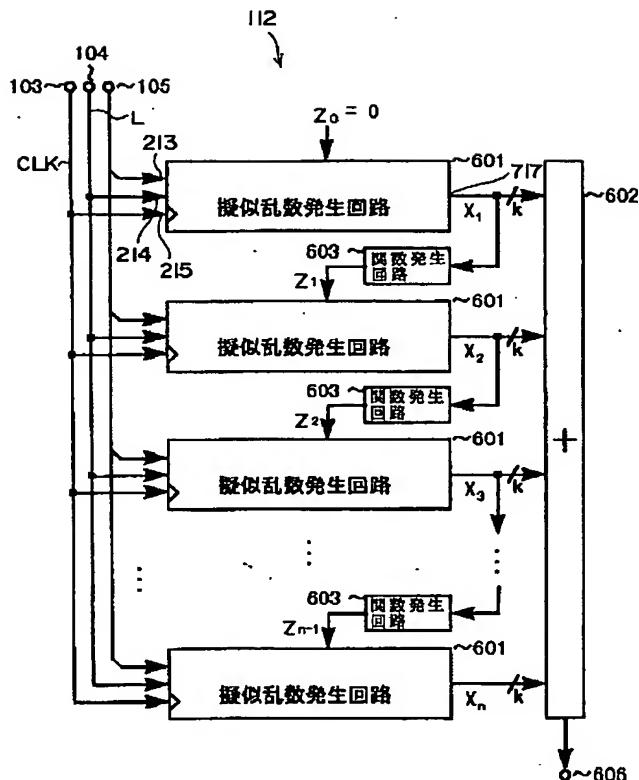
【図3】



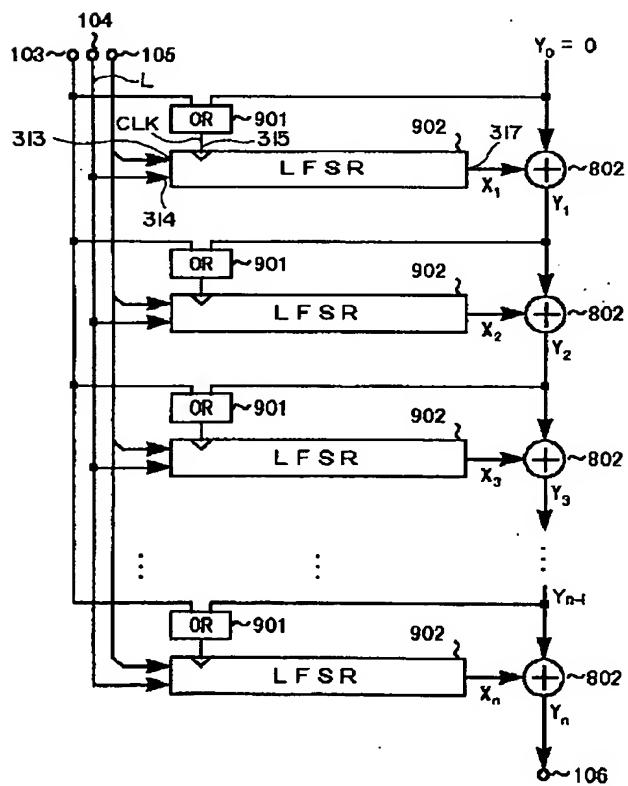
【図4】



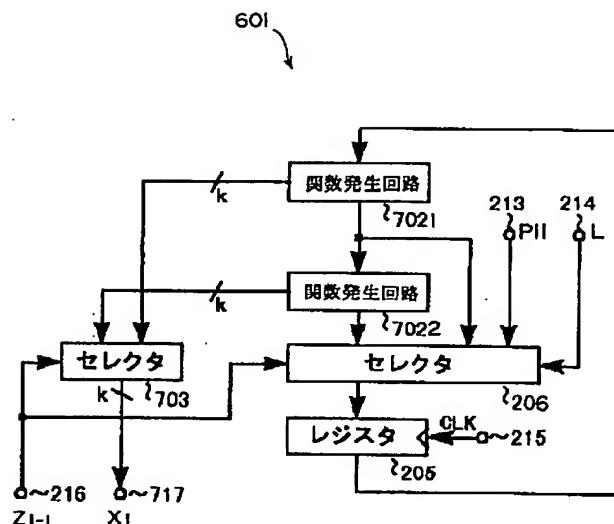
〔図5〕



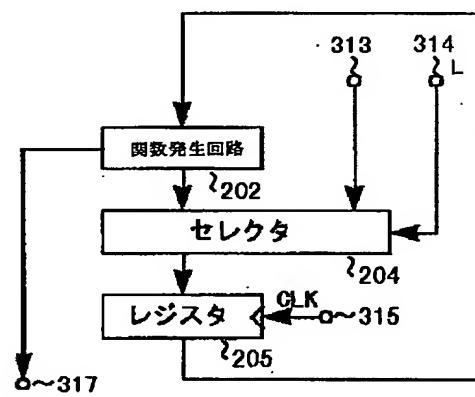
[図 7]



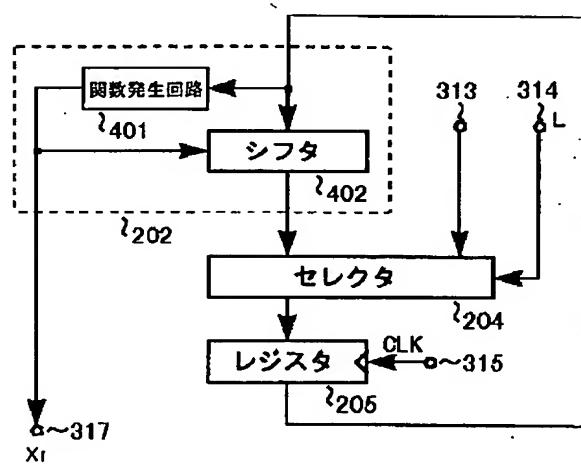
【図6】



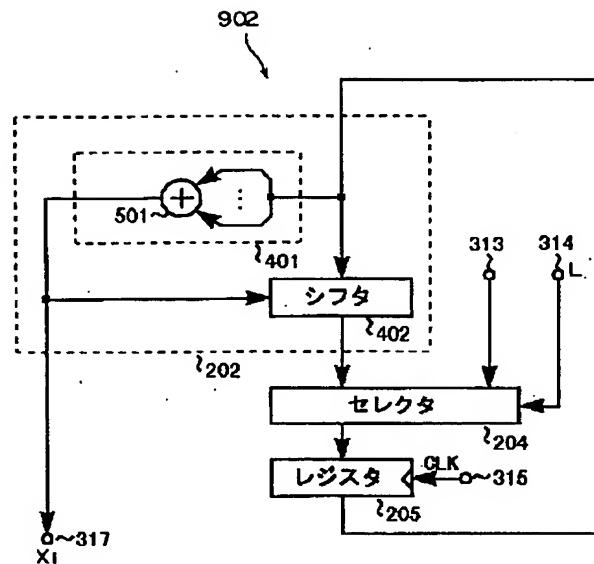
(图 8)



[図9]



【図10】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.